UNITED STATES PATENT APPLICATION

FOR

TUNNEL INTERWORKING

INVENTORS:
SUHAIL NANJI
BILL PALTER

PREPARED BY:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1026

(408) 720-8598

"Express Mail" mailing label number: EL 627446445US
Date of Deposit: 10/27/00
I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231
Leah Resendez
(Typed or printed name of person mailing paper or fee)
Leah Resendez
(Signature of person mailing paper or fee)
10-27-00
(Date signed)

TUNNEL INTERWORKING

BACKGROUND OF THE INVENTION

Field of the Invention

This invention relates to communication networks. More specifically, the present invention relates to interworking communication protocols.

Description of the Related Art

Virtual private networks (VPNs) have became a solution for extended corporate networks. VPNs are implemented with tunneling protocols. Tunneling protocols are also employed in the wholesale business model of a network provider. Tunneling conceals an Internet Service Provider's (ISP's)customer's network traffic from the network provider servicing the ISP. Protocols for tunneling evolve with changing requirements and technology. Moreover, new tunneling protocols are introduced with improvements over older protocols. Business decisions can lead companies to either select or reject a given protocol.

For example, the most popular tunneling protocol to implement VPNs currently is the Layer 2 Tunneling Protocol (L2TP). In addition, certain Internet Service Providers (ISPs) have made a decision to implement L2TP in their networks. A network provider, such as a telecommunications company (telecom), servicing corporations utilizing VPNs or ISPs selecting L2TP as the tunneling protocol of choice must conform to the selection or not service customers choosing L2TP.

Figure 1 (Prior Art) illustrates a network provider only servicing an ISP customer with a specific tunneling protocol and not servicing a different ISP selecting a different tunneling protocol. As Figure 1 illustrates, subscribers 101 access networks through a network provider 103. The network provider 103 can be any telecom or carrier. The network provider typically has numerous network elements such as routers, hubs, switches,

subscriber management systems, etc. In Figure 1, one of the telecom's network elements 105 is illustrated. The network element 105 can terminate the sessions from the subscribers 101 and tunnel the subscriber sessions to an ISP 109. The tunnel 107 between the network provider 103 and the ISP 109 is a tunneling protocol supported at the telcom's network element 105 and the ISP's network element 111. A different ISP 113 employs a different tunneling protocol on its network element 115. The ISP terminates a tunnel 117 from a different network provider which supports the tunneling protocol selected by the ISP 113. The network provider 103 cannot service the ISP 113 as a customer unless it supports the ISPs selected tunneling protocol.

Figure 2A (Prior Art) illustrates session switching. In Figure 2A, a network element 201 establishes a tunnel 203 to another network element 205 which is the tunnel endpoint. In this example, the tunnel 203 carries a subscriber session 202. The subscriber session 202 is tunneled again from network element 205 to a network element 209. The tunnel 207 between the network elements 205 and 209 is implemented with the same tunneling protocol as the tunnel between network elements 201 and 205. The network element 209 terminates the subscriber session.

Figure 2B (Prior Art) illustrates the network element 205 of Figure 2A switching the subscriber session 202 with the same tunneling protocol. As illustrated by Figure 2B, the tunnel 201 of Figure 2A is terminated at the network element 205. The subscriber session 202 first goes through an authorization sequence. A forwarding process 215 processes a first packet or control packet. A tunnel decapsulation routine 217 in the forwarding process 215 decapsulates the control packet from tunnel encapsulation. The decapsulated packet is then processed by a session decapsulation routine 216. The control packet is then processed by a payload decapsulation routine 219. Control information (e.g., subscriber, domain, etc.) from the control packet is passed to a control process 221. The control process 221 determines if the subscriber transmitted over the session 202 is authorized on the network element. For authorized subscribers, the control process 221 directs the forwarding process 215 how to

handle traffic from the session 202. After a control packet is received, data packets begin to arrive at the network element. The data packets are L2TP data packets encapsulating data payloads. If the session 202 is to be tunneled out, then the forwarding process 215 no longer passes payloads to the payload decapsulation routine 219. Instead, after the session decapsulation routine 216, payloads from the session 202 are passed to a session encapsulation routine 218 and then to a tunnel encapsulation routine 223. After tunnel encapsulation, the payloads for session 202 are transmitted out another session 204 through the tunnel 207.

A network provider could update their systems to support new tunneling protocols if a network provider would be willing to send people out to the field to update all of their functioning systems. After updating their systems to support the new tunneling protocol, the network provider would have to recertify all of their systems to comply with telecom regulations. Whenever a new tunneling protocol becomes a solution or a valued customer selects an unsupported protocol, the network provider would have to repeat these tasks. Session switching can terminate a session coming over a first tunnel and switch the session to be transmitted out another tunnel, but session switching is limited to the same tunneling protocol.

SUMMARY OF THE INVENTION

The invention provides an apparatus and method for tunnel interworking. A method for switching a subscriber session from a first tunneling protocol to a second tunneling protocol is provided herein.

In one embodiment of the invention, a subscriber session is received with a first tunneling protocol. According to the invention, if the subscriber session is to be transmitted with a second tunneling protocol then a session structure is created indicating the second tunneling protocol. The session is transmitted as indicated by the session structure.

In an alternative embodiment of the invention, a subscriber session is received with a first tunneling protocol. The session is includes data packets encapsulated with the first tunneling protocol. A payload is decapsulated from the data packets and the payload is decapsulated. A subscriber is indicated by the decapsulated payload and a set of data is retrieved corresponding to the subscriber. The set of data indicates the subscriber session is to be transmitted out a different tunnel with a different tunneling protocol. The different tunneling protocol is selected and the payloads are encapsulated with the different tunneling protocol directly after being decapsulated from the first tunneling protocol.

These and other aspects of the present invention will be better described with reference to the Detailed Description of the Preferred Embodiment and the accompanying Figures.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention may best be understood by referring to the following description and accompanying drawings that are used to illustrate embodiments of the invention. In the drawings:

Figure 1 (Prior Art) illustrates a network provider only servicing an ISP customer with a specific tunneling protocol and not servicing a different ISP selecting a different tunneling protocol.

Figure 2A (Prior Art) illustrates session switching.

Figure 2B (Prior Art) illustrates the network element 205 of Figure 2A switching the subscriber session 202 with the same tunneling protocol.

Figure 3A is a diagram illustrating a network element switching a subscriber session from one tunneling protocol to a different tunneling protocol according to one embodiment of the invention.

Figure 3B is a diagram illustrating the network element 305 of Figure 3a switching the session 302 from the tunnel 307, out the tunnel 309 with a different tunneling protocol according to one embodiment of the invention.

Figure 4 is a flowchart for switching a session between two different tunneling protocols according to one embodiment of the invention.

DETAILED DESCRIPTION OF THE DRAWINGS

The present inventions provides for interworking a session between different tunneling protocols. In the following description, numerous specific details are set forth to provide a thorough understanding of the invention. However, it is understood that the invention may be practiced without these specific details. In other instances, well-known protocols, structures and techniques have not been shown in detail in order not to obscure the invention.

Figure 3A is a diagram illustrating a network element switching a subscriber session from one tunneling protocol to a different tunneling protocol according to one embodiment of the invention. In the example of Figure 3A, a network provider 301 owns two network elements 303 and 305. The network element 303 originates a tunnel 307 which is terminated at the network element 305. The tunnel 307 is implemented with a tunneling protocol A (such as PPTP, L2F, L2TP, etc.). The network element 303 may only support tunneling protocol A. A subscriber session 302 is transmitted over the mandatory tunnel (i.e., a tunnel not generated by a subscriber) 307 from network element 303 to network element 305. In an alternative embodiment, the tunnel 307 could be generated from a subscriber (i.e., a voluntary protocol).

The network element 305 determines the destination network element for the session 302. In the example of Figure 3A, the network element 305 is selecting an ISP 315 or an ISP 313. As illustrated, the network element 305 determines that the session 302 is to be transmitted over another tunnel to the ISP 313. The ISP 313 supports the tunneling protocol

B which is a different tunneling protocol than tunneling protocol A. The network element 305 establishes a tunnel 309 to the ISP's network element 311 with tunneling protocol B. The session 302 is switched to a session 308 and transmitted over the tunnel 309 to the ISP 313. Thus, the network element 305 owned by the network provider 301 can switch an incoming session to either ISP 315 or ISP 313 independent of the tunneling protocol being supported by either ISP.

It should be understood other situations in which tunnel interworking can be used are within the scope of the invention. For example, one or more of the network elements owned by the ISPs 313 and 315 may instead be owned by the network provider. As another example, the network element 311 need not terminate the circuit, but may transmit the session to yet another network element through another tunnel. As another example, the network elements 311 may be owned by an entity other than a ISP (e.g., a corporation). As another example, the network element 303 may not be owned by the network provided.

Figure 3B is a diagram illustrating the network element 305 of Figure 3a switching the session 302 from the tunnel 307, out the tunnel 309 with a different tunneling protocol according to one embodiment of the invention. As illustrated by Figure 3B, the network element 305 of Figure 3A receives the subscriber session 302 over the incoming tunnel 307. The subscriber session 302 includes a series of packets, each packet having a payload. The first packet in the series of packets is a control packet for authenticating a subscriber. A control process 325 receives data from an authentication process 327. The data for the subscriber will indicate that the session 302 is to be transmitted out the tunnel 309. The data also indicates the tunneling protocol for the tunnel 309 which is different than the protocol of the tunnel 307. Control process 325 commands the forwarding process 329 to switch the session 302 out the egress tunnel 309 and indicates the different tunneling protocol for tunnel 309. Upon receiving the command, the forwarding process 329 sends the decapsulated payloads from the session 302 directly from the session decapsulation 316 to a session

decapsulation 318. The session decapsulation routine 381 passes traffic to a tunnel routine 331.

In the example illustrated by Figure 3B, only two tunneling protocols are illustrated although any number of tunneling protocols can be supported by the network element 305. Tunnel routine 331 selects the protocol encapsulation routine indicated by the control process 325 and encapsulates the decapsulated payloads with the selected tunneling protocol. For example, if the ingress tunnel 307 is implemented with a tunneling protocol A and the control process indicates that the egress tunnel 309 is implemented with a tunneling protocol B, then the tunnel process 331 will select the protocol B encapsulation routine 337 to encapsulate the decapsulated payloads of the subscriber session 302. After encapsulation, the forwarding process 329 transmits the subscriber session 302 over the egress tunnel 309 as a new subscriber session 308.

The decapsulation and tunneling routines can be implemented in any number of ways. These processes can be independent processes running on a network element. These independent processes would be governed and managed by a control process. In another implementation, the processes could be threads of a single process. The processes could also be independent modules. Although a number of implementations for this aspect of the invention have been described, they are only described to illustrate examples and not meant to be limiting on the invention.

Figure 4 is a flowchart for switching a session between two different tunneling protocols according to one embodiment of the invention. At block 401 of Figure 4, a packet is received over a session of an ingress tunnel. The network element decapsulates a payload from the packet of the session being transmitted over the tunnel with a first tunneling protocol at block 403. At block 405, the network element determines if the session is to be tunneled out of the network element. If the session is not to be tunneled out, then at block 407 the network element terminates the session and processes packets normally If the session is to be tunneled out, then at block 406 it is determined if the session is established.

If the session is not established, then at block 408 a request is made for the control process to establish the session. After block 408, control flows to block 401. If the session is established, then at block 409 looks up the session structure for the egress session. The session structure indicates the egress tunnel and the encapsulation of the egress tunnel. At block 413, the network element encapsulates the decapsulated packets of the ingress session as indicated by the created session structure for the egress tunnel at block 413.

In an alternative embodiment, the network element would have a table indicating supported tunneling protocols and their location. Functions or routines for some protocols would be supported locally while other protocols would be supported remotely. The owner of the network element could conserve memory while expanding protocol support by selecting a limited number of popular or frequently encountered tunneling protocols to be supported locally. The functions and routines to perform encapsulation and decapsulation for these selected protocols would be stored as images or modules locally. Additional protocols would be supported remotely by storing the decapsulation and encapsulation routines for these additional protocols on remote servers. If a locally supported protocol is needed for encapsulation or decapsulation, the network element could execute or call the functions or routines for the locally supported protocol. If a remotely supported protocol is needed for encapsulation or decapsulation of network traffic, the network element could remotely execute the functions or routines or temporarily import images or files to perform encapsulation and/or decapsulation.

Tunnel interworking enables a network provider (or other entity with a need for this ability) to carry network traffic between different tunneling protocols. The network provider can provide service to ISP customers regardless of the tunneling protocol received and the tunneling protocol selected by the ISP customer. A telecom acting as a network provider can avoid the complex task of adding protocol support to existing network elements with a single network element. The telecom's network infrastructure can still use the protocol supported on their network elements. Instead of recertifying and installing new or upgraded protocol

support at each network element in the telecom's network infrastructure, the telecom can install a network element implementing the invention at an access point between the telecom network and a service provider's network.

The techniques shown in the figures can be implemented using code and data stored and executed on computers. Such computers store and communicate (internally and with other computers over a network) code and data using machine-readable media, such as magnetic disks; optical disks; random access memory; read only memory; flash memory devices; electrical, optical, acoustical or other form of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.); etc. Of course, one or more parts of the invention may be implemented using any combination of software, firmware, and/or hardware.

While the invention has been described in terms of several embodiments, those skilled in the art will recognize that the invention is not limited to the embodiments described.

The method and apparatus of the invention can be practiced with modification and alteration within the spirit and scope of the appended claims. The description is thus to be regarded as illustrative instead of limiting on the invention